

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

**IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ARIZONA**

United States of America,

Plaintiff,

vs.

Elmer Guy Smith,

Defendant.

CR-09-0441-TUC-CKJ-DTF

REPORT AND RECOMMENDATION

Pending before the Court are Defendant's Motions to Suppress Evidence (Doc. No. 28) and to Dismiss the Indictment Due to Destruction of Evidence (Doc. No. 27). The government responded in opposition to these motions. (Doc. Nos. 36, 37.) Defendant replied. (Doc. Nos. 43, 44.) This matter came before Magistrate Judge Ferraro for a hearing and a report and recommendation as a result of a referral, pursuant to LRCrim 5.1. Defendant's motions were set for evidentiary hearing and evidence was heard on March 23, 24, and 25, 2010. Defendant was present and represented by counsel. This matter was submitted following oral argument at the conclusion of the hearing and taken under advisement.

Defendant's motions seek to suppress evidence Defendant claims was unlawfully seized by the government and dismiss the indictment because the government failed to preserve evidence material to the defense. The Magistrate Judge recommends that the

1 District Court, after its independent review, DENY Defendant's Motion to Suppress
2 Evidence and DENY Defendant's Motion to Dismiss the Indictment.

3 **I.**

4 **FACTUAL FINDINGS**

5 The Cincinnati division of the Federal Bureau of Investigation (FBI) sent an
6 investigative lead to FBI Special Agent (SA) Brian Hooton regarding several emails
7 containing child pornography which had been sent in 2002 to Defendant's email address.
8 (RT 3/23/10 at 15-19.) On May 15, 2008, SAs Brian Hooton and Travis Wilson went to
9 Defendant's home to follow up on this lead. (*Id.* at 19, 23.) Defendant was not at home
10 when the agents arrived, but Defendant's wife, Deirdre Smith, was home. (*Id.* at 23.) The
11 agents identified themselves, showed Mrs. Smith their credentials and explained to her that
12 they were investigating child pornography that had been sent to her husband's email address.
13 (*Id.* at 20, 24.)

14 At the evidentiary hearing, Mrs. Smith admitted that when the FBI agents came to her
15 house investigating child pornography she was shocked and her head was spinning. (RT
16 3/25/10 at 19-20.) She invited them inside because she did not want any of her neighbors
17 overhearing their conversation. (*Id.* at 6.)

18 The agents learned that Defendant and Mrs. Smith shared a computer and they
19 requested permission from Mrs. Smith to search the computer for child pornography. (RT
20 3/23/10 at 26, 95; RT 3/25/10 at 7.) At the evidentiary hearing, Mrs. Smith acknowledged
21 that she had mixed feelings about granting consent to search the computer. (RT 3/25/10 at
22 22.) On the one hand she wanted to know whether her husband had a sexual interest in
23 children, on the other hand she was unsure whether her husband would be okay with the
24 agents seeing the computer. (*Id.*) Mrs. Smith explained to the agents that she would be more
25 comfortable if her husband were present. (*Id.* at 9, 23.) The agents suggested that Mrs.
26 Smith call her husband's cell phone and speak with him. (*Id.* at 10-11, 23.) Although Mrs.
27 Smith believed her husband would not answer his cell phone while working she made at least

1 one attempt to call him. (*Id.* at 10-11.) Mrs. Smith was unable reach her husband. (*Id.* at 11.)
2 According to SA Hooton, he advised Mrs. Smith several times that she did not have to
3 consent to the search and that she could change her mind after consenting and terminate the
4 search. (RT 3/23/10 at 27, 29.) SA Hooton told Mrs. Smith that another agent, SA Eric
5 Campbell, had brought software that would be used to electronically search the computer.
6 (*Id.* at 28.) This software would only search for child pornography, not for personal or
7 financial information such as the text content of an email. (*Id.* at 27-28, 58, 128.) Mrs. Smith
8 consented to the computer search and SA Campbell was brought into the house to conduct
9 the forensic exam.¹ (*Id.* at 28.)

10 Mrs. Smith led the agents back to the computer room. (RT 3/25/10 at 13.) Mrs.
11 Smith told them that she thought her husband's Windows account/user name was password
12 protected. (*Id.* at 14.) Nevertheless, she logged out of her account/user name and then
13 selected her husband's account from the desk top. (*Id.*; RT 3/23/10 at 14, 30.) She
14 discovered it was not password protected. (RT 3/25/10 at 14; RT 3/23/10 at 30, 31.)

15 Upon discovering the account/user name was not password protected, the agents again
16 asked Mrs. Smith's consent to search the computer. (RT 3/23/10 at 31-32.) SA Hooton
17 handed Mrs. Smith a consent to search form and requested her signature. (*Id.* at 31.)
18 Initially, Mrs. Smith said she did not want to sign the form, but after the agents told her they
19 could not search the computer without her signature, she signed. (*Id.* at 32.) The consent
20 form clearly explained the equipment to be searched and that the agents had advised her of
21 her right to refuse consent to search. (Ex. 2.)²

22 The computer search was conducted by SA Campbell using ADF Triage, a forensic
23 computer program. (RT 3/23/10 at 127.) An electronic photograph has a unique hash value.

25 ¹ SA Campbell had been waiting in his car. (RT 3/23/10 at 19, 29.)

26 ² "Ex." refers to the exhibits submitted for the evidentiary hearing in this
27 Court. The exhibit lists are Doc. Nos. 61, 62.

1 (*Id.* at 127-28.) The ADF search program electronically searched the computer hard drive
2 for any identical or close matches to the hash values of known child pornography. (*Id.* at
3 128.) An electronic report of the search and all items found within the search parameters
4 were saved to SA Campbell's thumb drive. (*Id.* at 131.) Defendant's computer was found
5 to contain two known child pornographic photographs. (*Id.* at 136.) These photographs were
6 stored in a computer file used for background images by the Window's Instant Messenger
7 program. (*Id.* at 139.) Although the live use of Window's Instant Messenger was password
8 protected, the files containing the child pornography were not. (RT 3/24/10 at 7-8, 119-20.)
9 The computer search took about 45 to 50 minutes. (RT 3/23/10 at 34, 46.) Notwithstanding
10 the pornographic images of children on the hard drive, the computer was not seized by the
11 agents. (*Id.* at 37.)

12 After the search was completed the agents discovered a thumb drive attached to the
13 computer through a USB hub. (*Id.* at 40, 101.) The thumb drive had not been searched and
14 the agents thought it might also contain child pornography. (*Id.* at 40, 43.) Mrs. Smith did
15 not know anything about the thumb drive. (*Id.* at 101.) Initially, the agents asked Mrs. Smith
16 to keep the thumb drive in her possession and she placed it in her purse. (*Id.* at 43; RT
17 3/25/10 at 16-17.) Immediately after the agents left Mrs. Smith's home they reconsidered
18 their decision to leave the thumb drive. (RT 3/23/10 at 43.) The agents were concerned that
19 if Mrs. Smith retained the thumb drive Defendant could destroy the device or remove any
20 criminal images that might be there. (*Id.* at 43, 102.) They again knocked on the front door
21 and asked Mrs. Smith's permission to take the thumb drive with them. (*Id.* at 102-03.) Mrs.
22 Smith consented and initialed the consent form, which was modified to reflect the taking of
23 the thumb drive. (RT 3/23/10 at 44-45, 103; Ex. 2.) She also signed a property receipt form
24 acknowledging the agents had taken the item. (RT 3/23/10 at 45; Ex. 4.)

25 Defendant called and spoke to SA Hooton that afternoon. (RT 3/23/10 at 47.) Agent
26 Hooton requested permission from Defendant to search the thumb drive, which Defendant
27 denied. (*Id.*) Agent Hooton then made an appointment to meet with Defendant the next day
28

1 to return the thumb drive. (*Id.*) The following day, Defendant came to the FBI offices to get
2 his thumb drive and consented to an interview. (*Id.* at 48, 87.) As a result of the interview,
3 the agents believed they had probable cause to obtain a search warrant for the thumb drive.
4 (*Id.* at 87; RT 3/24/10 at 24-25.) The thumb drive was not returned to Defendant and the
5 agents obtained a search warrant for it. (RT 3/23/10 at 87-88.)

6 William Hajeski Jr. was a member of the FBI's Computer Analysis Response Team
7 (CART).³ (RT 3/24/10 at 47-48.) He was assigned the task of analyzing the thumb drive.
8 (*Id.* at 50.) When examining electronic media, a CART examiner tries to write block the
9 media, which protects the data from any changes. (*Id.* at 49-50.) His objective with the
10 thumb drive was to create a mirror image of the media and then retrieve any images or video
11 from the duplicate. (*Id.*) Mr. Hajeski Jr. discovered the drive was encrypted and he could
12 not access any data on it. (*Id.* at 51, 53; Ex. 8.) SA Campbell provided him a password from
13 Defendant, but Mr. Hajeski Jr. still was unable to get into the drive. (RT 3/24/10 at 33, 53;
14 Ex. 8.) Using a second password, he was no longer receiving the wrong password message
15 but it did not decrypt the drive. (RT 3/24/10 at 54-55.) During this process, he was using
16 write block software. (*Id.*; Ex. 8.) His numerous efforts to access the data on the drive were
17 unsuccessful. (RT 3/24/10 at 53-55.) He then attempted to write protect the data using
18 specially designed hardware. (*Id.* at 55; Ex. 8.) Again, his attempt failed. (RT 3/24/10 at
19 55; Ex. 8.) He entered the password without write protection and then added the write
20 protection before attempting to access the data, but this effort also failed. (RT 3/24/10 at 56;
21 Ex. 8.) Because none of the procedures provided access to the drive, Mr. Hajeski Jr. decided
22 to obtain an image of the drive without write protection. (RT 3/24/10 at 56-57; Ex. 8.)
23 Consequently, all of the relevant access dates on the thumb drive were changed to reflect the
24 search date as the last access date. (RT 3/24/10 at 59-60; Ex. 8.) The prior access dates can

25
26 ³ Mr. Hajeski Jr. has a Masters Degree in computer information systems and
27 two years on-the-job training with the FBI in forensic computer analysis. (RT 3/24/10 at
28 48.)

1 not be recovered. (RT 3/24/10 at 67.)

2 The thumb drive search revealed numerous pornographic images of children,
3 including one of the images found on the computer. These images are charged in the
4 indictment. (Doc. No. 1.) The images found on Defendant's computer were not alleged in
5 the indictment, except for the one duplicate image on the thumb drive.

6 II.

7 DISCUSSION

8 Defendant moves for suppression of all evidence obtained from his computer and
9 thumb drive and dismissal of the indictment due to destruction of evidence. The government
10 responds that the computer search and thumb drive detention were lawfully based upon Mrs.
11 Smith's voluntary consent, there were exigent circumstances to seize the thumb drive, and
12 the subsequent thumb drive search was conducted pursuant to a valid search warrant. The
13 government argues the changed access dates caused by the unprotected search of the thumb
14 drive was inadvertent.

15 A. CONSENT

16 A warrantless search is unconstitutional unless the government demonstrates that it
17 "fall[s] within certain established and well-defined exceptions to the warrant clause." *United*
18 *States v. Murphy*, 516 F.3d 1117, 1120 (9th Cir. 2008). The government asserts the
19 warrantless search of Defendant's computer and the detention of his thumb drive were
20 lawfully based upon voluntary consent of Deirdre Smith, Defendant's wife. Government
21 agents may conduct a search without a warrant or probable cause based upon an individual's
22 consent, so long as that consent was voluntary and came from someone authorized to give
23 it. *Schneckloth v. Bustamonte*, 412 U.S. 218, 222 (1973); *United States v. Matlock*, 415 U.S.
24 164, 172 n.7 (1974). Defendant asserts that Mrs. Smith's consent to search the computer and
25 to seize the thumb drive was involuntary and unauthorized.

26 1. Voluntariness

27 The government has the burden of proving by a preponderance of the evidence that
28

1 consent to a search was voluntary. *See Schneckloth v. Bustamonte*, 412 U.S. at 222; *United*
2 *States v. Matlock*, 415 U.S. at 177. Whether or not consent was voluntary or was the product
3 of coercion is determined from the totality of all the circumstances. *See Schneckloth*, 412
4 U.S. at 227; *Pavao v. Pagay*, 307 F.3d 915, 919 (9th Cir. 2002).

5 In this circuit there are five factors to be considered in determining voluntariness:

6 (1) whether the [consenting individual] was in custody; (2) whether the
7 arresting officers had their guns drawn; (3) whether Miranda warnings were
8 given; (4) whether the [consenting individual] was notified that she had a right
not to consent; and (5) whether the [consenting individual] had been told a
search warrant could be obtained.

9 *United States v. Brown*, 563 F.3d 410, 415 (9th Cir. 2009). “These factors serve merely as
10 guideposts, ‘not [as] a mechanized formula to resolve the voluntariness inquiry.’” *Id.*
11 (quoting *United States v. Patayan Soriano*, 361 F.3d 494, 502 (9th Cir. 2004)).

12 Defendant argues that Mrs. Smith’s consent was not voluntary because the record
13 demonstrates she attempted to refuse consent and her will was eventually overborne by the
14 agents’ persistence. According to Mrs. Smith, she told the agents “No” 20 times, but they
15 kept asking her “and rewording things to ask me the same thing over again and I did not want
16 to. And I would kind of say well yeah, because I was getting real uptight and I was very
17 nervous.” (RT 3/25/10 at 9-10.) “It took about 45 minutes of them asking and re-asking and
18 me, you know, not coming – not being clear and because I didn’t want them to.” (*Id.* at 12.)
19 According to SA Wilson, Mrs. Smith never said “no, you can’t search it. She never said you
20 need to wait until my husband is home.” (RT 3/23/10 at 118.) SA Wilson testified that they
21 asked permission to search numerous times “because every time we asked her, there was
22 never a concrete answer, it was never no and it was never yes, it was well, I don’t know, I’d
23 feel more comfortable if my husband were here, well, I’m not sure, it was those kinds of
24 answers.” (*Id.*) At the evidentiary hearing, Mrs. Smith admitted her responses to the agents’
25 requests to search were equivocal, “sometimes [she] would say no and sometimes [she]
26 would say yes.” (RT 3/25/10 at 10.) She acknowledged that she had mixed feelings about
27 granting consent to search the computer. (*Id.* at 22.)

The Court credits the agents' testimony over Mrs. Smith's regarding the time and nature of questioning before Mrs. Smith consented to the computer search. All three agents independently recalled the time to be no more than 15 minutes. (RT 3/23/10 at 28, 46, 95, 124.) Mrs. Smith admitted she was very nervous, had forgotten some things and did not even remember signing the consent form. (RT 3/25/10 at 12-13, 27.) Neither the length of time that elapsed prior to Mrs. Smith's consent nor her failure to promptly unequivocally consent demonstrate that her consent was coerced. To the contrary, numerous other factors establish she voluntarily consented.

The record reveals that Mrs. Smith was not in custody and it was a non-hostile environment. With respect to whether a person’s liberty has been so restrained that they are considered to be “in custody,” the Ninth Circuit looks at five factors:

(1) the number of officers; (2) whether weapons were displayed; (3) whether the encounter occurred in a public or non-public setting; (4) whether the officer's officious or authoritative manner would imply that compliance would be compelled; and (5) whether the officers advised the detainee of his right to terminate the encounter.

United States v. Brown, 563 F.3d at 415. Here, FBI agents came to Defendant's house in plain clothes. (RT 3/23/10 at 24, 91.) Only two agents came to the front door. (*Id.*; RT 3/25/10 at 5.) No weapons were visible (RT 3/23/10 at 80, 91). *See United States v. Crapser*, 472 F.3d 1141, 1149 (9th Cir. 2007) (consent voluntary though defendant in custody because officers did not have weapons drawn.) When Mrs. Smith answered the door both agents identified themselves and explained they were there investigating her husband's possible receipt of child pornography. (RT 3/23/10 at 24-25, 91-92.) Accordingly, Mrs. Smith knew immediately that she was not the target of their investigation. She invited the two agents into her home and led them into her kitchen. (RT 3/25/10 at 6). Mrs. Smith was not restrained and she never asked the agents to leave. (*Id.* at 27, 28; RT 3/23/10 at 29, 96, 99.) Mrs. Smith admitted it was not a hostile situation; the agents were polite, never raised their voices and never threatened her. (RT 3/25/10 at 13, 24.) The agents also found Mrs. Smith to be cooperative (RT 3/23/10 at 28-29, 93). *United States v. Rosi*, 27 F.3d 409, 412

1 (9th Cir. 1994) (“courts have inferred consent from the cooperative attitude of a defendant.”).

2 The agents testified that they advised Mrs. Smith numerous times that she had a right
3 to refuse their search request and could withdraw her consent and terminate the search even
4 after it had begun. (RT 3/23/10 at 29, 32, 64 95, 119.) Mrs. Smith acknowledged it was her
5 signature on the consent form, which clearly advised she had a right to refuse consent. (RT
6 3/25/10 at 12, 26; Ex. 2.)⁴ Knowledge of the right to refuse consent is highly relevant in
7 determining whether a consent is valid. *United States v. Mendenhall*, 446 U.S. 544, 558-59,
8 (1980).

9 The fact that Mrs. Smith initially did not want to sign the consent to search form (RT
10 3/23/10 at 97) is not dispositive. *See North Carolina v. Butler*, 441 U.S. 369, 375-76 (1979)
11 (refusal to sign a waiver form does not conclusively demonstrate that there was no waiver).
12 In particular, when the agents explained they could not search the computer unless she
13 signed, Mrs. Smith chose to sign the consent form (RT 3/23/10 at 32-33, 97-98). *United*
14 *States v. Castillo*, 866 F.2d 1071, 1082 (9th Cir. 1989) (execution of a consent form is one
15 factor that indicates that consent was voluntary). Based on the totality of circumstances, the
16 Court finds the government has established by a preponderance of the evidence that Mrs.
17 Smith voluntarily consented to the search of the computer.

18 After the computer search was complete, the agents asked for Mrs. Smith’s consent
19 to take a thumb drive they had found attached to a USB hub. It is uncontested that Mrs.
20 Smith gave them permission to take this item. (*Id.* at 44-45, 117, 120-21; RT 3/25/10 at 18-
21 19, 30.) The agents added the thumb drive to the consent form, and Mrs. Smith inscribed her
22 initials for the addition, and they gave her a property receipt for it. (RT 3/23/10 at 44-45,
23 117; RT 3/25/10 at 18, 30; Exs. 2, 4.) Accordingly, the Court finds the government has

25 ⁴ The consent to search form included an acknowledgment that she had “been
26 advised of [her] right to refuse to consent to this search” and that she was giving
27 permission for the search “freely and voluntarily, and not as a result of threats or
28 promises.” (Ex. 2.)

1 established by a preponderance of the evidence that Mrs. Smith voluntarily consented to the
2 detention of the thumb drive. The Court now turns to whether Mrs. Smith's consent was
3 authorized.

4 2. Authority to Consent

5 A third party's consent to the search of another's belongings is valid if the consenting
6 party has either actual or apparent authority to give consent. *United States v. Davis*, 332 F.3d
7 1163, 1169 (9th Cir. 2003). The government always bears the burden of proving consent.
8 *United States v. Guzman*, 852 F.2d 1117, 1122 (9th Cir. 1988); *United States v. Impink*, 728
9 F.2d 1228, 1232 (9th Cir.1984). "[W]hen the prosecution seeks to justify a warrantless
10 search by proof of voluntary consent . . . [it] may show that permission to search was
11 obtained from a third party who possessed common authority over or other sufficient
12 relationship to the premises or effects sought to be inspected." *United States v. Matlock*, 415
13 U.S. at 171. Common authority is not implied from the third party's property interest, rather,
14 actual authority to consent to a search of a container exists "if the owner of the container has
15 expressly authorized the third party to give consent or if the third party has mutual use of the
16 container and joint access to or control over the container." *United States v. Davis*, 332 F.3d
17 at 1169 (quoting *United States v. Fultz*, 146 F.3d 1102, 1105 (9th Cir.1998)); *United States*
18 *v. Matlock* at 171 n.7.

19 According to Mrs. Smith, both the computer and the thumb drive belonged to her
20 husband. (RT 3/25/10 at 10, 16.) The government offered no evidence to refute Mrs.
21 Smith's claim. Because the record demonstrates that Mrs. Smith did not have her husband's
22 express authorization to consent to the computer search and the detention of the thumb drive,
23 the government must show mutual use and joint access or control in order to demonstrate
24 actual authority.

25 The record clearly establishes Defendant and Mrs. Smith mutually used and had joint
26 access to the computer. Mrs. Smith testified that she told the agents she shared the computer
27 with her husband. (RT 3/25/10 at 7, 20.) The computer was located in a bedroom which she
28

1 and Defendant called “the computer room.” (*Id.* at 22.) Mrs. Smith’s access to the computer
2 was unlimited; she used the computer whenever she wanted to play games, read the news,
3 and to receive and send emails. (*Id.* at 14, 23.) Before the agents searched the computer,
4 Mrs. Smith logged out of her account/user name and clicked on Defendant’s page. (*Id.* at 14,
5 25.) Although Mrs. Smith believed Defendant’s account/user name was password protected,
6 it was not. (*Id.*) Neither were the images of child pornography that were found on the
7 computer hard drive. (RT 3/24/10 at 8.) Accordingly, she had joint access to all areas of the
8 computer she consented to be searched. Mrs. Smith had actual authority to consent to the
9 type of search conducted on the computer.

10 According to Mrs. Smith, she did not know what a thumb drive was. (RT 3/25/10 at
11 17, 29-30.) The agents asked her if the thumb drive belonged to her and she said it did not.
12 (*Id.* at 17.) At the time it was discovered, the thumb drive was attached to a USB hub next
13 to the computer. (RT 3/23/10 at 40, 101.) Given Mrs. Smith’s unlimited physical access to
14 the thumb drive she had actual authority to give it to the agents for safe keeping, but she
15 lacked authority to consent to its search.⁵

16 The agents reached the same conclusion – that Mrs. Smith lacked actual authority to
17 consent to a search of the thumb drive – and did not search the drive. (RT 3/23/10 at 44-45.)
18 Later that day, when SA Hooton requested Defendant’s permission to search the thumb drive,
19 Defendant refused and made an appointment to pick it up. (RT 3/23/10 at 47-48.) At the
20 time Defendant came to pick up the thumb drive he consented to an interview with the
21 agents. (*Id.* at 48.) Based upon Defendant’s statements in this interview, SA Hooton kept
22 the thumb drive and obtained a search warrant it. (*Id.* at 87-88; RT 3/24/10 at 24-25.)
23 Defendant has not alleged his statements were involuntary or that the search warrant was
24 invalid. Accordingly, the Court finds no basis to suppress the contents of the thumb drive.

25
26 ⁵ The contents of the thumb drive were encrypted. (RT 3/24/10 at 51.)
27 Hence, Defendant had taken special steps to protect the contents from the scrutiny of
28 others. *See* 4 Wayne R. LaFave, Search and Seizure 168 (4th ed. 2004).

1 3. Exigent Circumstances

2 Absent a finding of consent, the government argues there were exigent circumstances
3 to seize the thumb drive. The Court agrees. The government agents feared Defendant could
4 destroy any evidence which might be on the thumb drive if he retained possession. (RT
5 3/23/10 at 40.) To establish exigent circumstances due to possible destruction of evidence
6 there must be probable cause to suspect that evidence is present. *United States v. Impink*, 728
7 F.2d 1228, 1231 (9th Cir. 1984). Here, the agents had come to Defendant's residence to
8 investigate information from another FBI office that an e-mail containing child pornography
9 had been sent to Defendant's email address years earlier. (RT 3/23/10 at 15-16; Ex. 1.)
10 When agents searched Defendant's computer they found two images of child pornography.
11 (RT 3/23/10 at 136.) The computer data showed that the images had been created the week
12 before the search. (RT 3/24/10 at 11.) At the time of the search, the thumb drive was
13 connected to the computer through a USB hub. (RT 3/23/10 at 40, 101.) In the agents'
14 experience, child pornography is often stored on thumb drives. (*Id.* at 40, 43, 100; RT
15 3/25/10 at 16-17.) The Court finds the agents had probable cause to believe evidence was
16 present on the thumb drive. Given the ease with which evidence could be altered or destroy
17 on the thumb drive, its seizure was justified based upon exigent circumstances.

18 **B. FAILURE TO PRESERVE EVIDENCE**

19 Defendant seeks to dismiss the indictment claiming the government agents failed to
20 preserve Defendant's computer and destroyed the access dates when they searched the
21 thumb drive. Defendant asserts "the government's agents violated their own procedures in
22 not seizing the computer evidence." (Doc. No. 27 at 7.) As to the thumb drive, Defendant
23 merely claims "[t]here is no explanation as to why they accessed it in such a way as to
24 destroy the file access dates." (*Id.* at 10.) However, "unless a criminal defendant can show
25 bad faith on the part of the police, failure to preserve potentially useful evidence does not
26 constitute a denial of due process of law." *Arizona v. Youngblood*, 488 U.S. 51, 58 (1989).
27 Bad faith must be shown even when the destroyed evidence "could [have] eliminate[d] the
28

1 defendant as the perpetrator.” *Illinois v. Fisher*, 540 U.S. 544, 548 (2004).

2 Defendant asserts that failure to seize the computer violated government policy, which
3 demonstrates bad faith. First, arguing that the government agents acted in bad faith under
4 these circumstances tests the limits of credulity. Stating the obvious, Defendant maintained
5 custody and control of his computer and could have preserved it for whatever evidentiary
6 value he believed it had. Second, Defendant did not put on evidence of, or prove the
7 existence of, a departmental policy at the hearing. Nor did Defendant cite any authority to
8 support the dismissal of the indictment under these circumstances and the Court has found
9 none. Hence, dismissal is inappropriate on this basis.

10 With respect to the destruction of access dates on the thumb drive, Defendant has not
11 shown the government agents acted in bad faith. William Hajeski Jr., an FBI forensic
12 computer expert, testified how he inadvertently changed the access dates:

13 Q [Carin C. Duryee] Okay. So how – at this point how many times
14 have you tried to write block and – and been unsuccessful?

15 A [William Hajeski Jr.] A total of three different methods; one
16 software write block on the whole time, one hardware write
17 blocking, and one turning the software write block off, but then
18 turning it back on once I had obtained permission to get onto the
19 thumb drive.

20 Q And – and are – and did you document these steps in your
21 notes?

22 A Yes.

23 Q Okay. So what did you do next?

24 A At that point I knew I had access to the thumb drive with the
25 write protection off, so I decided to turn the write protection off
26 and obtain an image that way.

27 Q And why did you decide to make an image without write block?

28 A Because at the time I didn’t think there was another way to
access the thumb drive.

Q Okay. What did you do then?

A In an attempt to see if the hard drive was recognized by the
operating system, I opened Windows Explorer and clicked on

1 the – the – the drive that was present to make sure it was there.

2 Q Tell us what you mean by drive, is that the H or –

3 A The thumb drive, sorry.

4

5 Q During the examination, at some point did you learn or see that
6 access dates had changed on some of the files?

7 A Yes.

8 Q How did you notice that or what brought it to your attention?

9 A Having – not having write protection on the media when I took
10 the image, one of the first things I checked was the access dates
11 because I had the ability to write to that thumb drive. So when
12 I sorted all the files by access dates, I noticed the date that I had
13 accessed the thumb drive on there, so I put that in my notes.

14 Q Okay. What was the date of this examination?

15 A June 6th of '08.

16

17 Q Okay. Do you know now how the access dates on the – how
18 many files was it, 93 files, how those were changed?

19 A When I – when I clicked on the drive letter to verify the drive,
20 was seen by the operating system with the thumbnails coming
21 up showing what the images were, the operating system would
22 have had to access that file to generate the thumbnail and I
23 believe at that point is when I changed the access dates.

24 Q Okay. Did you realize that was happening as you opened or as
25 you checked to see if the drive was there?

26 A At the moment my intention was to just verify the drive was
27 there. I inadvertently generated the thumbnails, so at that very
28 moment I didn't realize I was accessing the files. It became
apparent to me once I sorted by the access dates.

Q And at the time that you removed write block after your
attempts and failures, did you think there was any way for you
to access that thumb drive with write block on?

A No.

(RT 3/24/10 at 56-57, 59-60, 64.) Defendant's own expert had no opinion on whether Mr.

Hajeski Jr. made a deliberate mistake or the changing of the access dates was inadvertent.

28

1 (RT 3/24/10 at 138.)

2 At best, Defendant has established the government altered the access dates
3 negligently. The negligent destruction of evidence does not violate due process. *Arizona*
4 *v. Youngblood*, 488 U.S. at 58; *United States v. Barton*, 995 F.2d 931, 936 (9th Cir. 1993).
5 Accordingly, Defendant's motion to dismiss the indictment for destruction of evidence must
6 fail.

7 **III.**

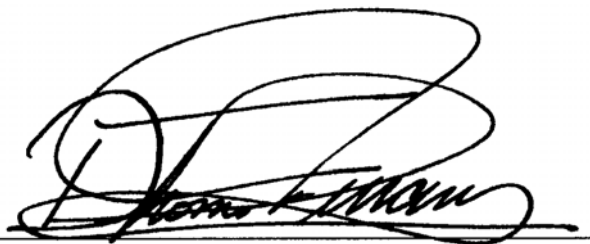
8 **RECOMMENDATION**

9 In view of the foregoing, it is recommended that, after its independent review of the
10 record, the District Court DENY Defendant's Motion to Suppress Evidence (Doc. Nos. 28)
11 and DENY Defendant's Motion to Dismiss the Indictment (Doc. No. 27).

12 Pursuant to Federal Rule of Criminal Procedure 59(b)(2), any party may serve and file
13 written objections within 14 days of being served with a copy of this Report and
14 Recommendation. If objections are not timely filed, they may be deemed waived. The
15 parties are advised that any objections filed are to be identified with the following case
16 number: **CR-09-441-TUC-CKJ**.

17 DATED this 19th day of April, 2010.

18
19
20
21
22
23
24
25
26
27
28

A handwritten signature in black ink, appearing to read "D. Thomas Ferraro", is written over a horizontal line.

D. Thomas Ferraro
United States Magistrate Judge